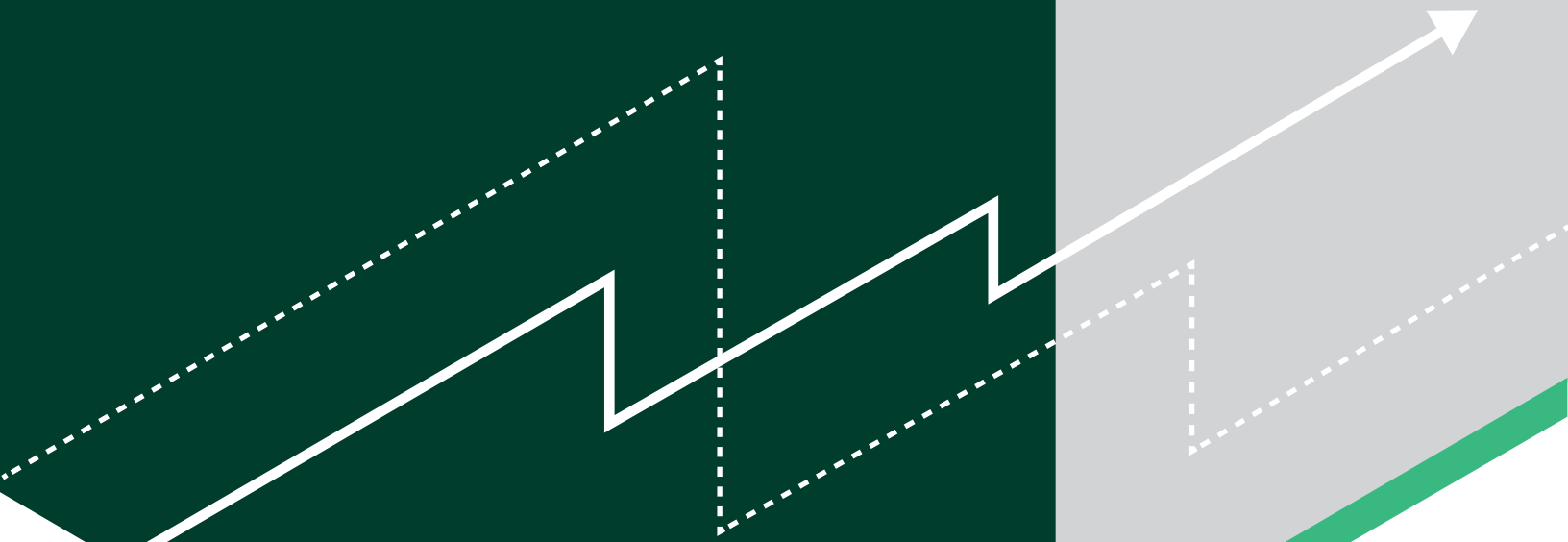
A Forrester Consulting
Thought Leadership Paper
Commissioned By BeyondTrust

November 2020

Evolving Privileged Identity Management (PIM) In The Next Normal

Secure Your Remote Workforce And Protect Your Business With PIM In The Post-COVID Era



FORRESTER®

Table Of Contents

Project Director:
Joshua Blackborow,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Security leaders must navigate these unprecedented and uncertain waters by rapidly changing, augmenting, and adapting their security systems to keep their organizations protected from threats.

Executive Summary

When it comes to security strategy and execution, the old adage is true: You're only as strong as your weakest link. Persistent attackers are looking for weak spots, and it only takes one for a successful breach.

The COVID-19 pandemic necessitated a massive and immediate move to remote work, accelerating a shift that was already in motion but previously happened with more foresight and planning. This accelerated shift has made organizations increasingly vulnerable with now larger-than-ever attack surfaces. Traditional privileged users (IT admins and others with powerful access to IT systems) are now working remotely, and traditional business users are requiring privileged access to perform their jobs from home. Corporate endpoints have moved to workers' homes, quickening the trend toward "identity as the new perimeter" and accelerating the adoption of zero trust approaches. Simultaneously, companies have expedited digital transformation initiatives, such as the shift to cloud, which is further disintegrating the traditional perimeter.

Security leaders must navigate these unprecedented and uncertain waters by rapidly changing, augmenting, and adapting their security systems to keep their organizations protected from threats. Relying on perimeter-based network security and legacy remote technologies like VPN for remote access does not provide the granular identity-based security that is needed when the workforce — and the apps, data, and infrastructure they are using — could be located anywhere.

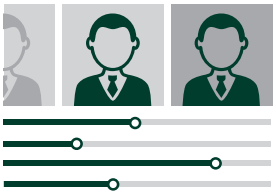
Privileged users also require additional access controls that still allow them to do their jobs and keep the entire remote workforce productive. Security leaders must rethink their privileged identity management (PIM) strategies to go beyond traditional password management and embrace the full spectrum of PIM, including endpoint privilege management and secure remote access.

BeyondTrust commissioned Forrester Consulting to evaluate PIM challenges in the new normal created by COVID-19. Forrester conducted an online survey with 320 IT and security decision-makers in North America, Europe, and Asia to explore this topic.

KEY FINDINGS

- **The rise in the remote workforce comes with considerable security risk.** Most decision-makers (83%) believe that the increase in remote workers has increased their attack surfaces and risk to vulnerabilities; nearly two-thirds say that their organizations are underprepared for the rise in remote workers.
- **PIM plays a key role in securing this increased attack surface.** The remote workforce is driving up the need for privileged access, which has increased the importance of PIM to security leaders. Over 90% of decision-makers agree that PIM plays a crucial role in securing remote workers.
- **Most PIM programs are still immature.** Few companies are taking a mature, holistic approach to PIM, including frequent rotation of both human and machine credentials, just-in-time (JIT) access controls, granular control and auditing over privileged remote access, and privilege escalation and delegation.

COVID-19 Has Accelerated The Need For PIM

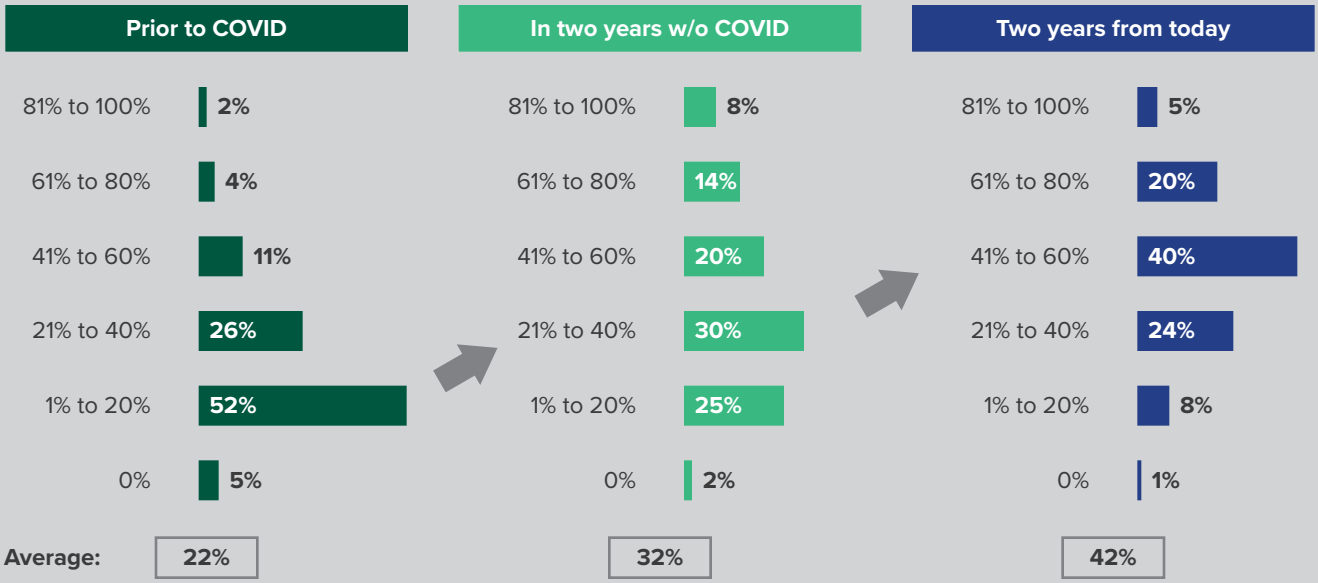


As the remote workforce expands, there is little question that PIM will play an increasingly crucial role in keeping companies safe. In our study, we found:

- **COVID-19 has accelerated the move toward a remote workforce.** Prior to the outbreak of this global pandemic, there was already a clear trend toward remote work. Security leaders believe that had COVID-19 not emerged, the remote workforce would have increased by 45% in the next two years. However, due to COVID-19, this has jumped to a 91% forecasted increase (see Figure 1).
- **An increasingly remote workforce creates a significant security risk.** A remote workforce presents a substantial number of security challenges. Eighty-three percent of respondents indicate that an increase in the remote workforce will increase their risk of security incidents (see Figure 2). Remote workers are more susceptible to scams, they create authentication challenges, and the proliferation of user-owned devices provides significant challenges as well.
- **Employees increasingly expect remote work.** Fifty-three percent of US workers reported wanting to work from home more even after the pandemic is over, according to Forrester's PandemicEX Survey.[1]

Figure 1

Percentage Of Workforce Who Are Primarily Remote Workers

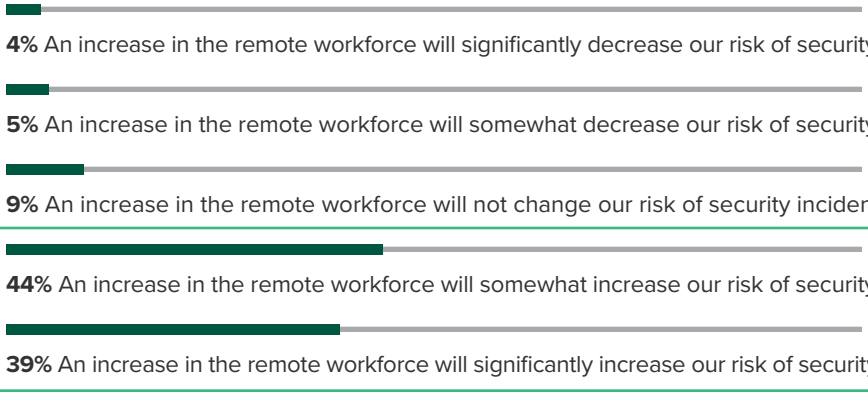


Base: 320 IT security and operations professionals in NA, EU, or APAC
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

FORRESTER®

Figure 2

"To what extent will an increase in remote workers change your organization's vulnerability to security incidents (e.g., data breaches, ransomware, DDoS attack)?"



4% An increase in the remote workforce will significantly decrease our risk of security incident.

5% An increase in the remote workforce will somewhat decrease our risk of security incident.

9% An increase in the remote workforce will not change our risk of security incident.

44% An increase in the remote workforce will somewhat increase our risk of security incident.

39% An increase in the remote workforce will significantly increase our risk of security incident.

Over 80% of decision-makers say their organizations are facing increased risk of security incident due to a larger remote workforce.

Base: 320 IT security and operations professionals in NA, EU, or APAC
Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

› **Unprepared for this change, organizations are left vulnerable to attacks.** Security leaders understand how crucial it will be to secure remote workers. In fact, respondents list preparing for an increasingly remote workforce as their number one priority for the next year. Despite this importance, nearly two-thirds of respondents say that their organizations are underprepared for a significant increase in remote workers from a security standpoint.

PIM IS KEY TO SECURING A REMOTE WORKFORCE

Securing privileged access in a dynamic business environment is a tough balancing act. Forrester estimates that at least 80% of data breaches are connected to compromised privileged credentials.[2]

91% of respondents agree that PIM plays a crucial role in securing remote workers.

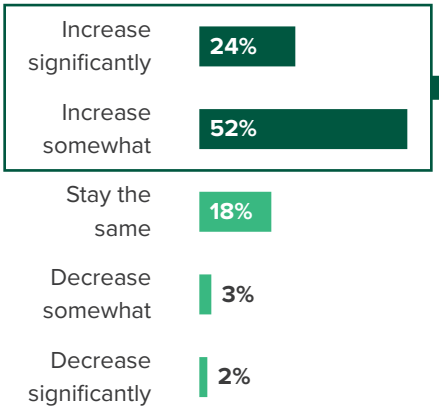
Most PIM decision-makers (76%) expect increases in the number of privileged sessions in their organizations over the next two years, while only 5% anticipate a decrease. This is due in part to the increase in remote workers. Sixty percent of respondents expect their privileged sessions to increase over the next two years because they must treat more employees as privileged to provide the remote access required to execute their jobs (see Figure 3).

When it comes to PIM, the increase in privileged users is the top challenge cited by respondents (see Figure 4). Traditional privileged users are some of the most difficult to manage; respondents cite IT admins as presenting the greatest vulnerability of any user when working from home. This – along with other factors such as an increase in privileged machine access (e.g., service accounts, robotic process automation) and increased scope of who is considered privileged – means that privilege management has more use cases to address, and is more important than ever.

In fact, 91% of respondents agree that PIM plays a crucial role in securing remote workers. You can see this reflected in firms' budget plans. Despite the economic downturn, 86% of respondents say that their organizations will invest *more* in PIM over the next two years, and only 2% will invest less.

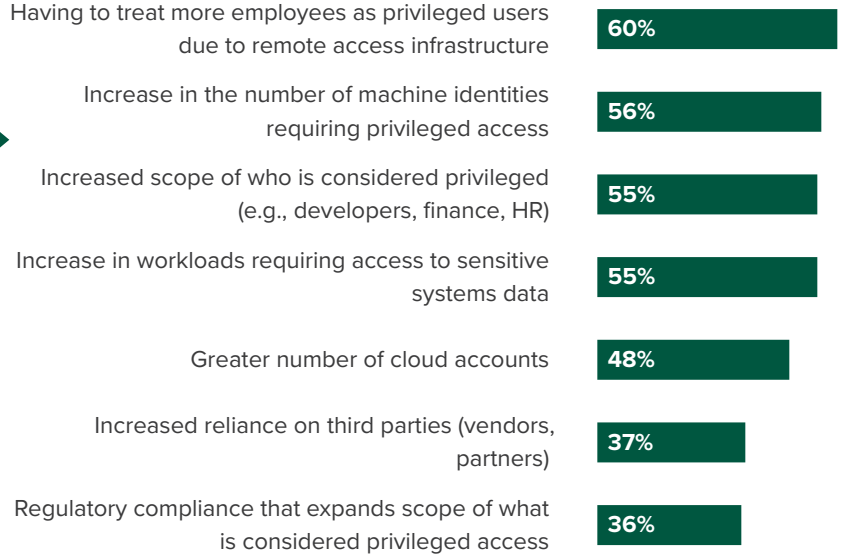
Figure 3

"How do you expect the number of privileged sessions (human or machine) within your organization to change in the next two years?"



Base: 320 IT security and operations professionals in NA, EU, or APAC
Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

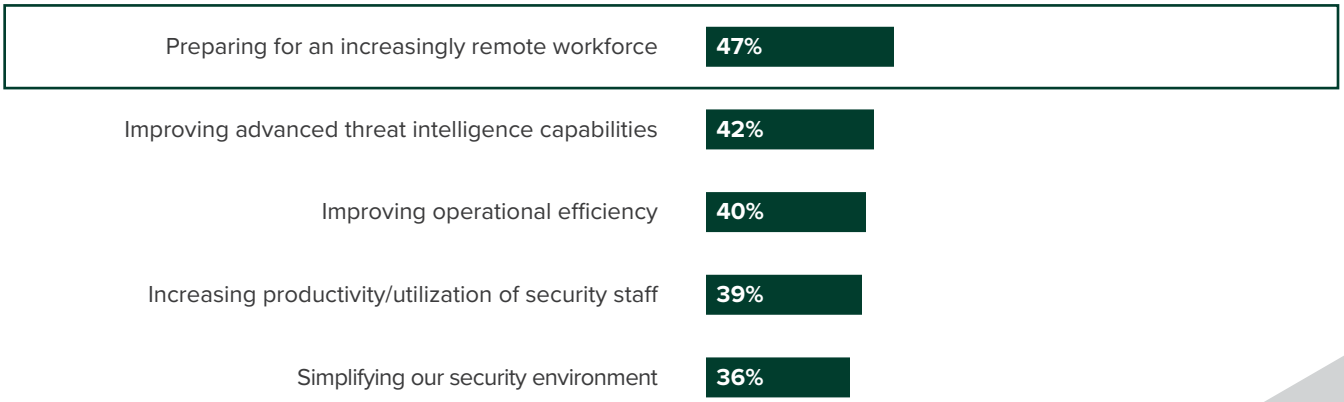
"Why do you expect the number of privileged sessions (human or machine) within your organization to increase in the next two years?"



Base: 241 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

Figure 4

"What are your organization's top security priorities for the next year?" (Sum of top five ranked)



Base: 320 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

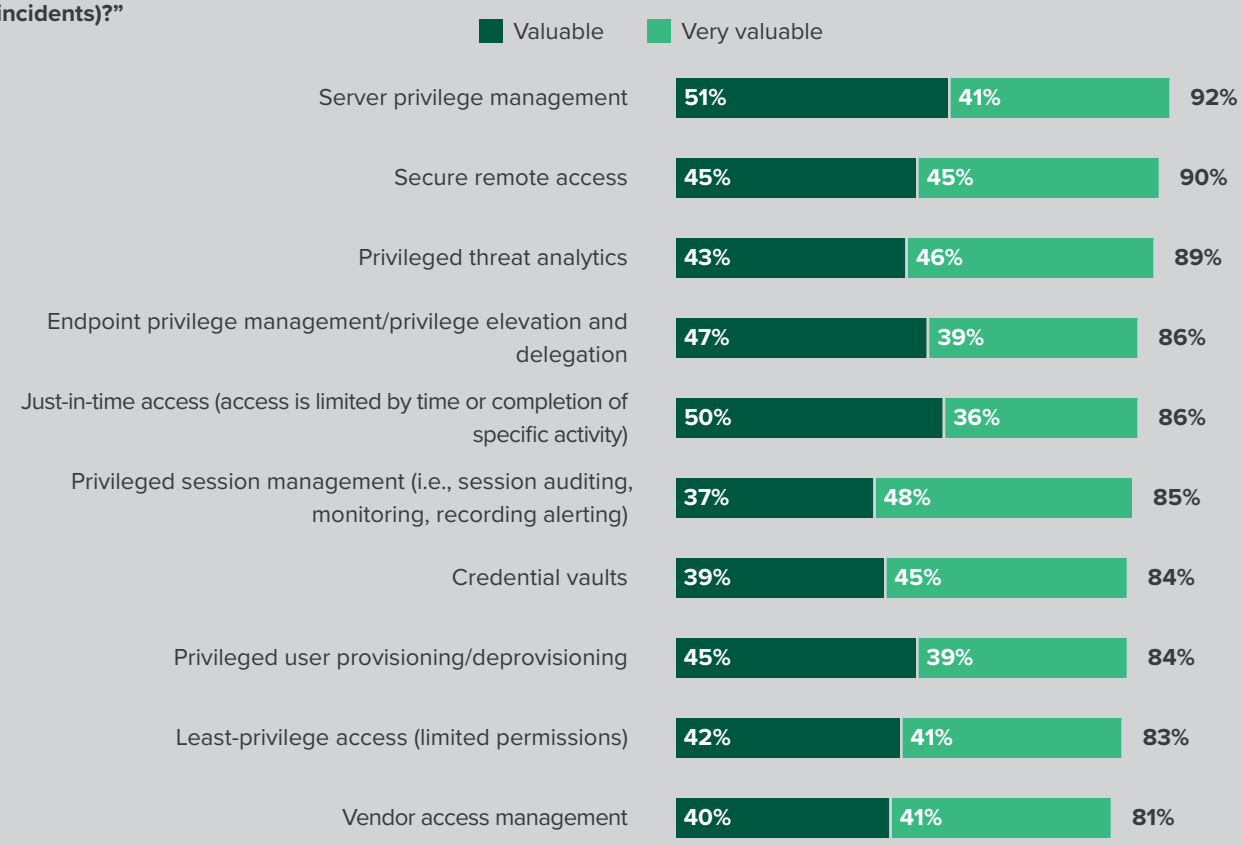
Shore Up Security And Drive Efficiencies With PIM

PIM plays a clear and vital role in properly securing, protecting, and limiting an organization's attack surface. Having an effective PIM suite provides considerable benefits to the security organization as well as the business. We found:

- **Comprehensive PIM is necessary to prevent many breaches.** Of the decision-makers whose organizations have suffered a security incident related to privileged user credentials, 92% state that server privilege management would have been valuable in preventing it. Ninety percent of respondents find secure remote access valuable in preventing privileged user credential incidents, and 89% feel this way about privileged threat analytics. In fact, PIM technologies/features receive high marks across the board: When it comes to preventing security incidents, no fewer than 81% of decision-makers consider PIM technology valuable (see Figure 5).

Figure 5

"You indicated that your organization has suffered a security incident related to privileged user credentials. How valuable do you believe each of the following PIM technologies/features could have been in preventing that incident (or multiple incidents)?"



Base: 150 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

FORRESTER®

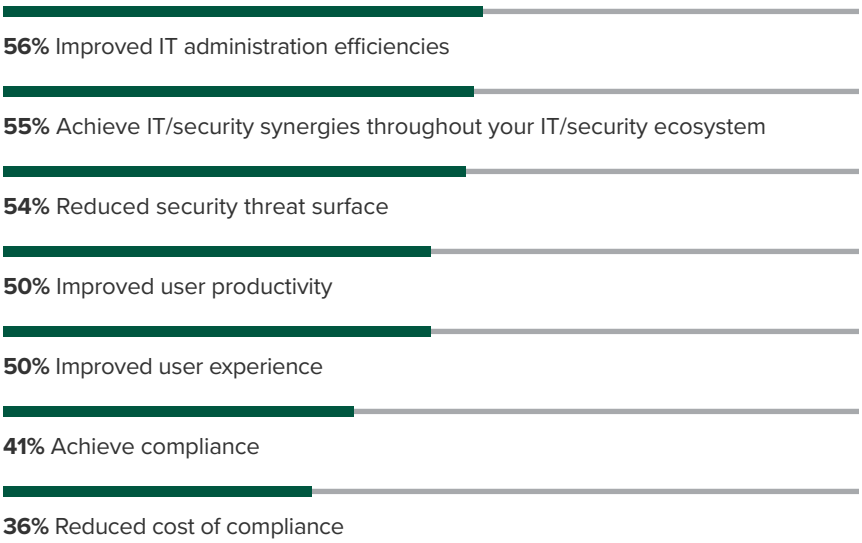
› **PIM comes with more than just improved security.** Even though organizations are dealing with lower budgets because of the economic downturn, security leaders realize the efficiency savings that PIM solutions can drive are an added value to the security protections. Decision-makers report that improved IT administration efficiencies (56%) is the top benefit of PIM, with IT system synergies (55%), improved user productivity (50%), and improved user experience (50%) also ranking highly (see Figure 6). The fact that an effective PIM solution leads to not only improved security, but also efficiencies across IT ecosystems, means that PIM, when done right, will provide a greater bang for your buck than other security solutions.

If you're not already investing in modernizing and expanding your PIM approach, then you're not doing enough to protect your organization from attack. The pandemic is not only creating net-new problems, but also accelerating, amplifying, and exposing pre-exisiting ones and demanding quick and methodical solutions.

The need for resiliency, security performance, and workforce productivity is more imperative than ever. Those organizations working to implement a complete and integrated PIM suite will be best poised to withstand new security challenges during and beyond the pandemic.

Figure 6

"Which of the following benefits can your organization achieve through implementing effective privileged identity management?"



Base: 320 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

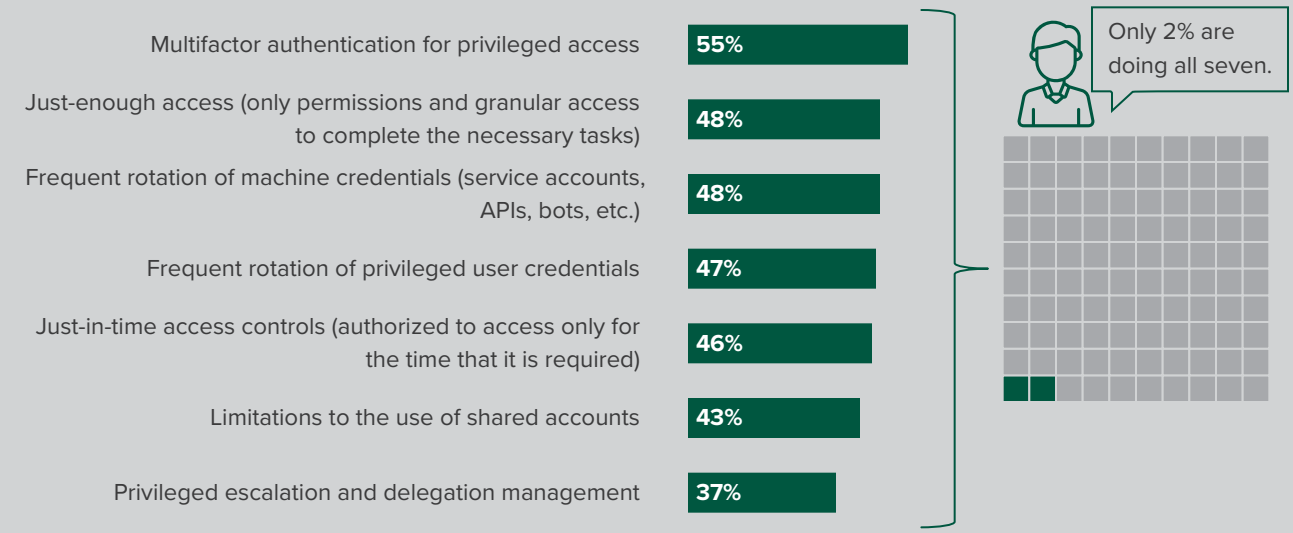
Organizations Struggle For Holistic PIM

The new normal has created more urgency for businesses to assert control over privileged access. Even prior to the increase in remote work, privileged users were a challenge for most organizations: Two-thirds of business leaders whose organizations have experienced a security incident in the past 24 months report undergoing an incident involving privileged accounts. Firms struggle with discovering all privileged accounts across the enterprise, integrating privileged access controls with IT service management and change management workflows, and securing all privileged credentials in the network. This is due in large part to immature and incomplete PIM practices. Our study found:

- **You're only as strong as your weakest link.** While many firms have implemented PIM point solutions on an ad hoc basis, only 41% of decision-makers say their organizations have deployed full PIM suites. This is troubling because attackers don't target the most secure surface of an organization; they actively pursue the weak points. Firms are falling into a false sense of security when they only have a few technologies implemented.
- **You must protect privileges across accounts, endpoints, and access pathways.** Attack surfaces for privileged access have expanded since the surge in remote working; shrinking them needs to be a top concern for organizations. This requires a holistic, multitiered approach. Even those who have a full PIM suite of technology are not taking all the necessary actions to reduce risk: Only 2% of decision-makers report their firms are executing all necessary steps to reduce their attack surfaces, with multifactor authentication for privileged access being the most common action taken (see Figure 7).

Figure 7

"What are you doing to limit the attack surface for privileged access in case an attacker can obtain privileged credentials?"



Base: 320 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

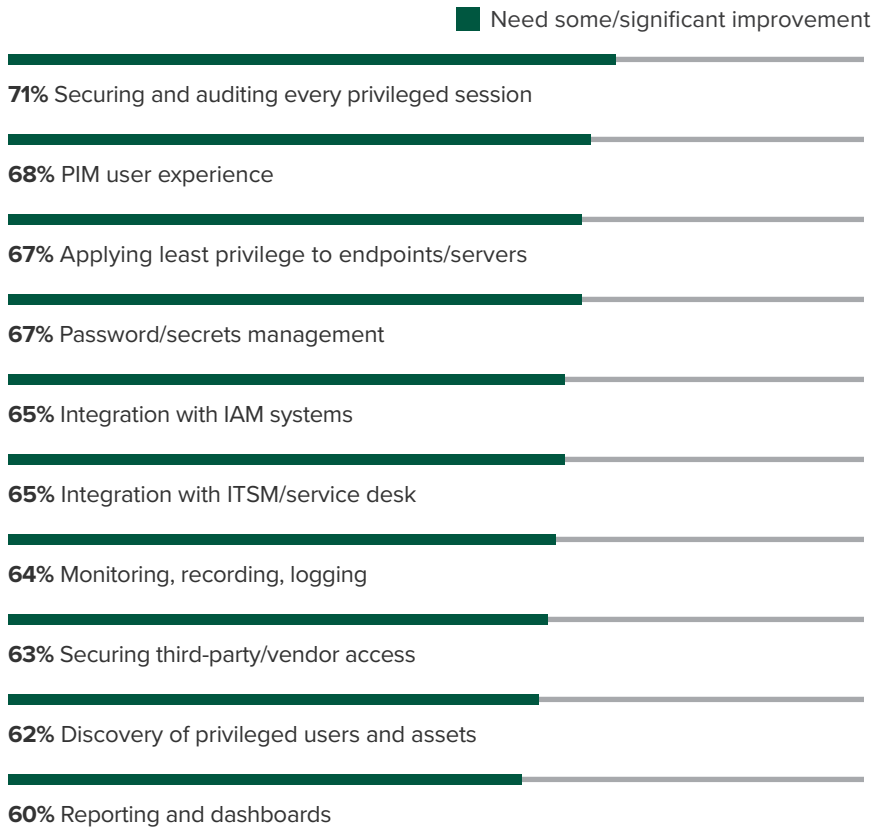
FORRESTER®

- **Solutions are poorly integrated and clunky.** Over half of IT decision-makers say their organizations manage privileged access either manually or with standalone solutions. Unsurprisingly, the top two challenges are poor integration with their IT/security ecosystems and reduced worker productivity. Well-integrated PIM platforms result in more seamless connection with the rest of the IT ecosystem and a more user-friendly workflow.
- **This leaves organizations with systems that aren't meeting standards.** These incomplete and poorly integrated PIM technology suites are leaving firms without much confidence in their PIM capabilities. Decision-makers need improvement in numerous areas related to privilege management, including securing and auditing every privileged session (71%), PIM user experience (UX) (68%), and applying least privilege to endpoints/servers (67%) (see Figure 8).

Over half of leaders say their organizations manage their privileged access either manually or with standalone solutions.

Figure 8

"To what extent do you believe your organization needs to improve each of the following areas of PIM?"



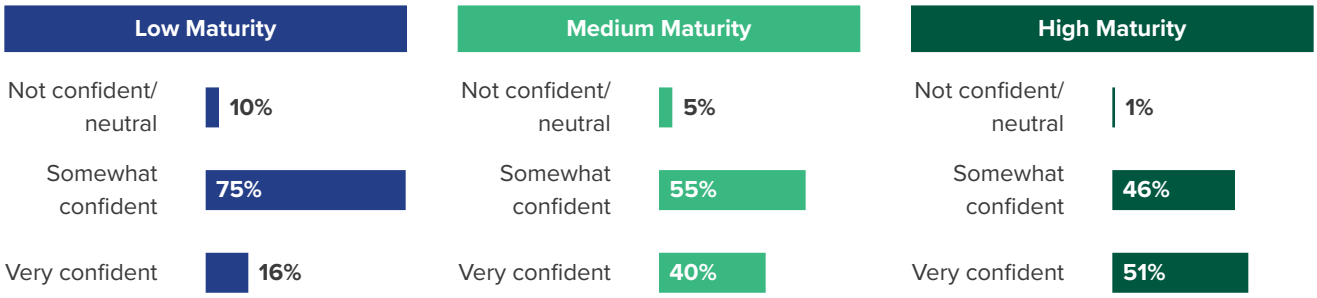
Base: 320 IT security and operations professionals in NA, EU, or APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

› **PIM allows organizations to limit and contain attacks.** Those who have a complete and integrated PIM suite report their companies are doing better in multiple areas than those with disjointed and ad hoc PIM technology solutions. To examine the effect of more mature PIM technology suites, we created a simple maturity model. Forrester categorizes respondents with a full suite of all eight key PIM technologies that are taking an integrated PIM platform approach as "high maturity," while those with neither the full suite nor the integrated approach are considered "low maturity." Those with either one or the other, or a partial suite, are considered "medium maturity." We found that decision-makers at high-maturity organizations are far more confident in their ability to limit threat surfaces and prevent escalating privileges that can cause mega breaches (see Figure 9).

With budgets tightening, it is becoming increasingly crucial to invest in an efficient and effective PIM suite. Time and cost of deployment and high costs are cited as the top barriers to expansion of PIM. These challenges, coupled with poorly integrated systems, leave organizations with bloated and inefficient PIM suites that are not meeting standards. Security decision-makers must focus on finding the right privilege management technology — and coupling that with effective processes, policies, and skill sets — to maximize their investments and improve their security postures.

Figure 9

"How confident are you that your organization has limited the threat surface so that, even if an attacker steals privileged credentials, they will not be able to move laterally or escalate privileges to inflict greater damage?"



Base: 320 IT security and operations professionals in NA, EU, or APAC
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

Key Recommendations

The seismic shift to remote work, brought on by COVID-19, has accelerated the trend toward zero trust and identity as the new perimeter. Remote work will drive up the number of privileged users and privileged sessions over the next two years. Privileged users are critical to the operations of digital business, yet as power users, they also present a grave security risk to organizations. Firms must put effective PIM controls in place to limit the attack surface while still enabling regular business operations.

Plan for the rising tide of remote privileged users. The rapid increase in human and machine privileged access will lead to many security blind spots and compliance violations. To avoid this, firms must set up the tools and processes to discover and categorize privileged users and activities to determine appropriate access rights and apply the security controls that best fit the needs of various privileged user types and situations, from traditional admins to third-party vendors to DevOps.

A strong governance model is essential for PIM. Standing access and full admin rights for privileged users are a critical subset of the overprovisioning problem. Traditional PIM tools don't effectively meet the rules and governance of privileged users; firms must evolve and expand their solutions to secure changing environments and attack surfaces.

Implement strategies to reduce the attack surface and prevent lateral movement. Adhere to the principle of least privilege (POLP) by granting privileged users just enough access to resources and just enough permissions to perform actions required for their jobs. Use a privileged escalation and delegation approach to give privileged users session-based access to resources that they only need periodically. Revoke unneeded access and automate the detective work for human and machine privileged access that is questionable.

Apply just-in-time (JIT) access approaches for dynamic business use cases. Privileged access must be nimble in certain parts of the business with a high rate of change in which personnel or machine identities must access resources. Limiting access to time-bound requests with context-aware workflows for approval removes standing access while enabling the business to march on.

Balance UX with security controls for remote privileged users. Security controls are vital, but don't secure yourself out of business. Users need privileged access to various systems and data to keep things running smoothly. Make the authentication and access request process as frictionless as possible. Employ unobtrusive security controls like session monitoring and threat detection that run in the background and can alert you to high-risk activities.

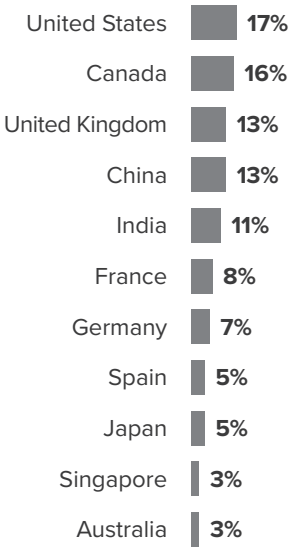
Provide centralized, consistent administration with an integrated PIM suite. Today's complex, hybrid environments have resulted in an explosion of privileges that malicious actors can target to gain access to and move laterally throughout an organization. Thus, firms need a modern, comprehensive set of PIM tools and approaches to protect the enterprise. While point solutions may provide some protections, full visibility of the threat level across the privileged landscape through an integrated platform provides consistent administration, reporting, and response capabilities.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 320 IT and security decision-makers in North America, Europe, and Asia to evaluate PIM. Survey participants included decision-makers in their organizations' identity and access management strategy who are involved in security and risk or identity management. Questions provided to the participants asked about privileged identity management, security, and how they're responding to an increasingly remote workforce. Respondents were offered a small monetary incentive as a thank you for time spent on the survey. The study took place in June 2020.

Appendix B: Demographics

COUNTRY



GEOGRAPHY

33% North America
34% EU
34% APAC

NO. OF EMPLOYEES

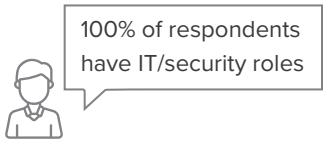
11% 500 to 999
47% 1,000 to 4,999
32% 5,000 to 19,000
11% 20,000+

SENIORITY

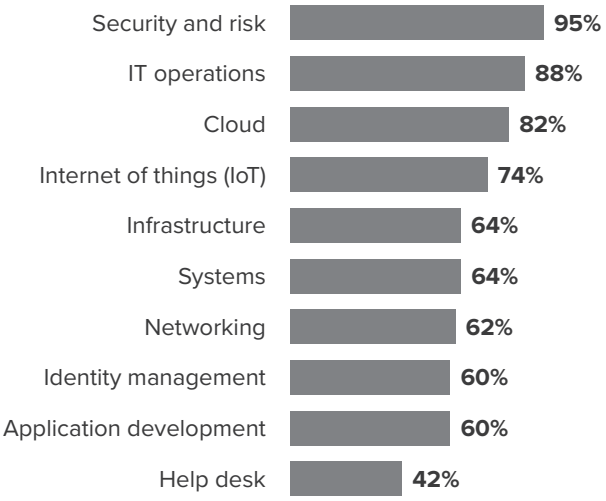
17% Senior manager
38% Director
9% Vice president
36% C-level executive

IDENTITY AND ACCESS MANAGEMENT RESPONSIBILITY

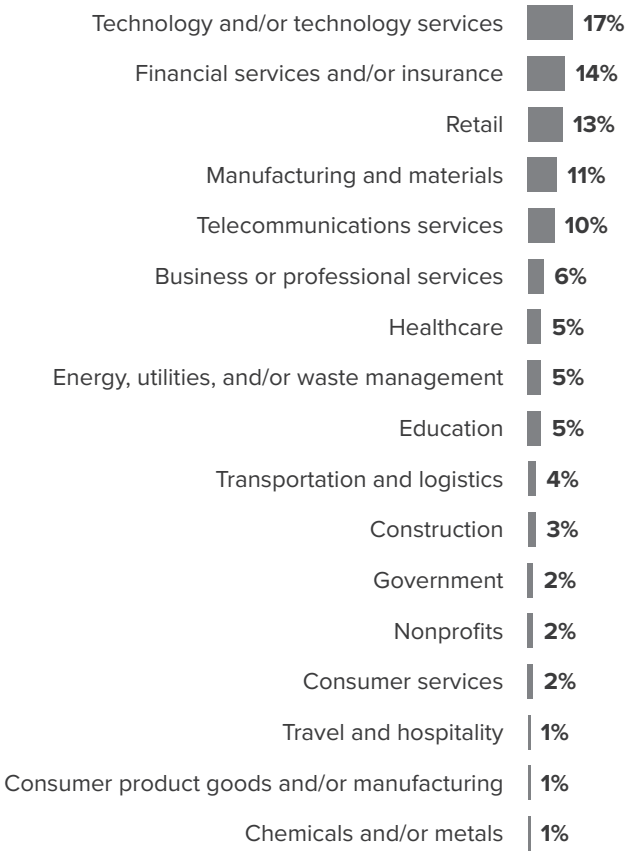
17% Decision-influencer
38% Part of team
9% Final decision-maker



IT/SECURITY INVOLVEMENT



INDUSTRY



Base: 320 IT security and operations professionals in NA, EU, or APAC
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

FORRESTER®

Appendix C

ENDNOTES

[1] Base: 338 respondents. Sources: "The State Of Remote Work, 2020," Forrester Research, Inc., July 6, 2020, and Forrester's Q2 2020 US PandemicEX Survey 2 (April 29 to May 1, 2020).

[2] Source: "The Forrester Wave™: Privileged Identity Management, Q4 2018," Forrester Research, Inc., November 14, 2018.